

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
A. <u>Consent</u> for Release of Health Information						
	Section 164.506 Consent for uses or disclosures to carry out treatment, payment, or health care operations					
1	Final rule requires consent for these purposes except in the following circumstances, provider has an indirect treatment relationship, individual is an inmate, in emergency treatment situations, law requires provider to treatment individual, attempts are made to obtain consent but barriers to communication exist and consent to receive treatment is inferred from the circumstances.	Do you obtain an individual's consent prior to using or disclosing PHI to carry out treatment, payment, or health care operations? (See regulation for implementation specifications and definition on PHI)	obtain copy of policy/procedure			
2	The regulation lists the requirements for a valid consent. See regulation for the list of these requirements.	Does your consent form meet the requirements of the HIPAA regulation?	obtain copy of policy/procedure			
3	Failure to obtain a consent must be documented. The documentation must contain information about the attempt to obtain consent and the reason why consent was not obtained.	Do you have a process in place to document failure to obtain a consent?	obtain copy of policy/procedure. Interview HIM, admitting/registration, ED, any department treating patient.			
4	An individual may revoke a consent at anytime except to the extent that action has already been taken based on the existing consent. The revocation must be in writing.	Do you have a process in place to allow individuals to revoke a consent?	obtain copy of policy/procedure. Interview HIM, admitting/registration, ED, any department treating patient.			
5	Signed consents must be documented and retained in original or electronic copy for six years from the date of creation or the date that it was last in effect, whichever is later.	Do you have a record retention process in place that includes these consents?	obtain copy of policy/procedure. Interview HIM, admitting/registration, business office/patient accounts, risk management			
6	If a conflict exist, use and disclosure must follow the most restrictive document. The conflict may be resolved by obtaining a new consent or communicating (orally or in writing) with the individual to determine the individual's preference. This preference must be documented and followed.	Do you have a process in place to resolve conflicts between consents and any other authorization or written legal permission for use/disclosure of PHI for payment, treatment, or healthcare operations?	obtain copy of policy/procedure. Interview risk management, compliance. Review established complaint process			
B. <u>Authorization</u> for Release of Health Information						
	Section 164.508 Uses and disclosures for which an authorization is required					
7	The regulation requires authorization for uses and disclosure of PHI other than those obtained under the consent for payment, treatment, and health care operations or otherwise allowed under the rule.	Do you have a policy and procedure for obtaining authorization for use and disclosure of PHI for purposes other than payment, treatment, or health care operations?	obtain copy of policy/procedure			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
8	The regulation spells out the core elements to an authorization as well as implementation specifications.	If yes to the above, does your authorization form meet the regulation requirements? (See regulation for a list of the requirements).	obtain copy of authorization			
9	(a)(2) Psychotherapy notes Specific individual authorization is needed before this information could be disclosed with a few exceptions. These exceptions are listed in the regulation.	Do you generate psychotherapy notes? If yes, are these notes shared with or disclosed to anyone? (See regulation for definition of psychotherapy notes.)	Interview HIM, psychiatric ward			
10	(b)(3) Compound authorizations Authorizations for use and disclosure of PHI may not be combined with any other document to create a compound authorization except under specific conditions. These conditions are listed in the regulation.	Do you ever use "compound" or combined authorizations?				
11	(b)(4) Prohibition on conditioning of authorizations Treatment, payment, enrollment in the health plan, or eligibility for benefits to an individual may not be conditioned on the provision of an authorization except under certain exceptions. See regulation for these exceptions.	Do you ever condition treatment, payment enrollment in the health plan, or eligibility for benefits on the provision of an authorization from an individual?	ED--EMTALA, interview admitting/registration, RN supervisors			
12	(b)(5) Revocation of authorizations An individual may revoke an authorization at anytime except to the extent that action has already been taken based on the existing consent, or if the authorization was obtained as a condition for obtaining insurance coverage, other law provides the insurer the right to contest a claim under the policy. The revocation must be in writing.	Do you have policies and procedures that allow for the revocation of an authorization?	obtain copy of policy/procedure			
13	(b)(6) Documentation Signed authorizations must be documented and retained in original or electronic copy for six years from the date of creation or the date that it was last in effect, whichever is later.	Do you have a documentation process in place that includes these authorizations?	obtain copy of policy/procedure			
C.	Opportunity to Agree with or Reject Uses of Information Is Required...					
	Section 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.					
	164.510(a) Use and Disclosure for Facility Directories					
14	The following PHI may be used in a facility directory: Individual's name, location within the facility, condition in general terms that does not communicate specific medical information, and religious affiliation.	Do you maintain a facility directory? If so, does your directory contain only the allowable PHI?	Interview admitting/registration, volunteers			
15	Disclosure of directory information is allowed to members of the clergy or to persons who, except for religious affiliation, ask for the individual by name.	Does your policy regarding your facility directory meet the requirements for disclosure to clergy and to persons asking for the individual by name?	Interview admitting/registration, volunteers, social services, pastoral care			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
16	An individual must be informed of the PHI that may be included in a directory, to whom the information may be disclosed, and provide the individual with an opportunity to restrict or prohibit some or all of the uses of the PHI.	Does your policy regarding your facility directory allow for the individual to restrict or prohibit some or all of the uses of directory information?	obtain copy of policy/procedure. Interview admitting/registration			
17	If an opportunity to object is not able to be provided due to an individual's incapacity or an emergency treatment situation. PHI may be used in a facility directory under certain guidelines. See regulation for these restrictions.	Does your policy regarding your facility directory allow for use or disclosure of PHI in the facility directory in emergency circumstances?	obtain copy of policy/procedure			
164.510(b) Use and Disclosure for Involvement in the Individual's Care and Notification Purposes						
18	(b)(1) Permitted uses and disclosures A covered entity may disclose to a family member, other relative, or close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the care of the disclosure is in accordance with certain requirements (See regulation for requirements).	Do you ever disclose PHI to a family member, other relative, or close personal friend of the individual?	Interview RNs in each unit, HIM, phone operator			
19	There are requirements to be met for disclosure depending upon whether or not the individual is present. (See regulation for requirements).	If yes to the above, does your disclosure policy meet the requirements of the regulation?	obtain copy of policy/procedure			
C. Opportunity to Agree with or Reject Uses of Information Is Required...(cont)						
164.510(b) Use and Disclosure for Involvement in the Individual's Care and Notification Purposes (cont)						
20	A covered entity may disclose PHI to notify, or assist in the notification (including identifying or locating) a family member, personal representative, or another person responsible for the individual's care of the individual's location, general condition, or death if the disclosure is in accordance with certain requirements (See regulation for requirements.)	Do you ever disclose PHI to notify, or assist in the notification (including identifying or locating) a family member, personal representative, or another person responsible for the individual's care of the individual's location, general condition or death?	Interview ER, social services, RNs			
21	There are requirements to be met for disclosure depending upon if the individual is present or not, or the disclosure is for disaster relief purposes. (See regulation for requirements).	If yes to the above, does your disclosure policy meet the requirements of the regulation? (See regulations for requirements).	obtain copy of policy/procedure			
22	A covered entity may use professional judgment and experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up these items, if the individual is not present or able to agree or object to the disclosure.	Do you ever allow persons to act on the behalf of individuals to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of PHI? If so does your disclosure policy meet the requirements of the regulation?	Interview HIM, radiology, pharmacy			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
D. Opportunity to Agree or Reject with Uses of Information is NOT Required...						
	Section 164.512 Uses and disclosures for which consent, an authorization, or opportunity to object is not required					
	164.512(b) Public Health Activities					
23	(b)(1)(i) General Public Health Activities This type of PHI may be disclosed to a health authority that is authorized by law to collect or receive such information for the purpose of preventing, or controlling disease, injury, or disability. Must be sure policy & procedures match regulation.	Do you ever release PHI for public health activities (I.e. surveillance, communicable disease investigations, registries, birth or deaths, produce defects or problems, adverse events, etc.)?	Government issue--obtain copy of policy/procedure, interview person involved with registries (tumor, head/spinal cord injury, etc.) RNs			
24	(b)(1)(ii) Child Abuse and Neglect This is not restricted, but do need to review process/policies to be sure match regulation.	Do you ever release PHI to an authority authorized by law to receive reports of child abuse or neglect?	Government issue--obtain copy of policy/procedure, interview ED			
25	(b)(1)(iii) Food and Drug Administration Disclosure is not restricted for the purpose of reporting adverse events, product defects/problems, or biological product deviations, or for tracking products, enable recalls, repairing, or replacement, or for conducting post marketing surveillance.	Do you ever release PHI to a person under the jurisdiction of the Food and Drug Administration?	Government issue--obtain copy of policy/procedure			
26	(b)(1)(iv) Communicable Disease Disclosure is not restricted if the covered entity is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.	Do you ever release PHI to persons who may have been exposed to a communicable disease or may otherwise be at risk for contracting or spreading a disease or condition?	Government issue--obtain copy of policy/procedure			
27	(b)(1)(v) Members of the Workforce This is allowed, with some restriction, if you are a provider who is a member of the employer's workforce or who provides health care at the request of the employer for medical surveillance of the workplace, or to evaluate if the individual has a work related illness or injury. (See regulation for restriction)	Do you ever release PHI to employers about a member of an employer's workforce?	Worker's Comp.-- obtain copy of policy/procedure			
D. Opportunity to Agree or Reject with Uses of Information is NOT Required...(cont)						
	164.512(c)-(I) Other					
28	(c) Victims of abuse, neglect, or domestic violence This is allowed, with some restrictions, if the disclosure is to a government authority, including social services or protective services authorized by law to receive such reports. (See regulation for restrictions.)	Do you ever disclose PHI about individuals you reasonably believe to be a victim of abuse, neglect, or domestic violence.	Victims of Violence policy--obtain copy of policy/procedure			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
29	(d) Health Oversight Activities Disclosure is allowed for these appropriate oversight activities. However, disclosure is not allowed if the individual is the subject of the investigation or activity AND the activity is not related to receipt of health care, a claim for public health benefits, or qualification for public benefits when the patient's health is integral to the claim for public benefits.	Do you ever release information for health oversight activities (I.e. audits, civil, administrative, or criminal investigations, licensure or disciplinary actions, etc.) for appropriate oversight of the health care system, Government benefit programs (where PHI is relevant to beneficiary eligibility), or entities subject to government regulatory programs or civil rights laws where PHI is needed to determine compliance?	Government issue--obtain copy of policy/procedure			
30	(e) Judicial and Administrative Proceedings A covered entity may disclose PHI in the course of judicial or administrative proceedings if certain conditions are met. (See regulation for conditions).	Do you ever release PHI in the course of any judicial or administrative proceedings?	obtain copy of policy/procedure			
31	(f)(1) Pursuant to Process and as Otherwise Required by Law Information may be disclosed to law enforcement pursuant to process and as otherwise required by law if certain conditions are met. (See regulation for conditions)	Do you ever release PHI to a law enforcement official pursuant to process and as otherwise required by law?	obtain copy of policy/procedure			
32	(f)(2) Limited Information for Identification and Location Purposes The following PHI may be disclosed: name & address; date & place of birth; social security number, ABO blood type & rh factor, type of injury; date & time of treatment; date and time of death; and description of distinguishing physical characteristics (including ht, wt, gender, race, hair/eye color, scars, tattoos, and facial hair). Except as permitted above, you may not disclose PHI related to DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue for purposes of location or identification.	Do you ever release PHI to a law enforcement official for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person	obtain copy of policy/procedure			
D. Opportunity to Agree or Reject with Uses of Information is NOT Required...(cont)						
	164.512(c)-(l) Other (cont)					
33	(f)(3) Victims of Crime Information may be disclosed to law enforcement about victims of a crime if certain conditions are met. (See regulation for conditions)	Do you ever release PHI to a law enforcement official about victims of a crime?	obtain copy of policy/procedure			
34	(f)(4) Decedents This type of disclosure is allowed if you have suspicion that the death may have resulted from criminal conduct.	Do you ever release PHI to a law enforcement official about a person who has died for the purpose of alerting law enforcement of the death of the individual?	obtain copy of policy/procedure			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
35	(f)(5) Crime on Premises Disclosures of PHI to a law enforcement official is allowed if you believe in good faith constitutes evidence of criminal conduct that has occurred on your premises	Do you ever release PHI to a law enforcement official about a criminal conduct that may have occurred on your premises?	obtain copy of policy/procedure			
36	(f)(6) Reporting Crime in Emergencies Disclosure of PHI in response to a medical emergency (except if the emergency is on your premises) is allowed if such disclosure appears necessary to alert law enforcement of the commission & nature of a crime; the location or such crime or victim; the identity, description, & location of perpetrator of such crime. If the medical emergency was the result of abuse, neglect, or domestic violence, you must follow the requirements related to that type of disclosure.	Do you ever release PHI to a law enforcement official, in the course of responding to a medical emergency, that may be related to criminal conduct?	obtain copy of policy/procedure			
37	(g)(1) Coroners and Medical Examiners Disclosure of PHI to coroners and medical examiners is allowed for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.	Do you ever release PHI information about deceased persons to coroners or medical examiners?	obtain copy of policy/procedure			
38	(g)(2) Funeral Directors Disclosure of PHI to funeral directors is allowed to the extent the disclosure is consistent with applicable law, as necessary for the directors to carry out their duties with respect to the decedent. If necessary the disclosure may be made prior to and in reasonable anticipation of the individual's death.	Do you ever release PHI information about deceased persons to funeral directors?	obtain copy of policy/procedure			
D. Opportunity to Agree or Reject with Uses of Information is NOT Required...(cont)						
	164.512(c)-(l) Other (cont)					
39	(h) Postmortem Organ, Eye, and Tissue Donation Disclosure of PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue is allowed, for the purpose of facilitating such donation or transplantation.	Do you ever release PHI information to organ procurement organizations or organizations engaged in similar functions for the purpose of organ, eye, or tissue donation and transplantation?	obtain copy of policy/procedure			
40	(i) Research Purposes Use and disclosure of PHI for research, regardless of the funding of the research is allowed, provided certain conditions are met. (See regulation for conditions).	Do you ever use or disclose PHI for research?	obtain copy of policy/procedure			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
41	(j) Serious threat to Health or Safety Disclosure of PHI to avert a serious threat to health or safety is allowed, provided certain conditions are met. (See regulation for conditions).	Do you ever use or disclose PHI for the purpose of averting a serious threat to health or safety?	obtain copy of policy/procedure			
42	(k)(1) Military and Veterans Activities Disclosure of PHI of Armed Forces personnel is allowed for the purpose of activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission. The military authority has had to have published a notice in the Federal Register that states who the appropriate military command authorities are and the purposes for which the PHI may be used or disclosed.	Do you ever use or disclose PHI of individual who are Armed Forces personnel?	obtain copy of policy/procedure			
43	(k)(1) Military and Veterans Activities These covered entities may disclose PHI of an individual who is a member of the Armed Forces to the Department of Veterans Affairs for the determination of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.	This is only applicable to covered entities who are components of the Departments of Defense or Transportation	obtain copy of policy/procedure			
44	(k)(1) Military and Veterans Activities These covered entities may disclose PHI to components of the Department of Veterans Affairs that determine eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.	This is only applicable to covered entities who are a component of the Department of Veteran Affairs	obtain copy of policy/procedure			
D. Opportunity to Agree or Reject with Uses of Information is NOT Required...(cont)						
	164.512(c)-(l) Other (cont)					
45	(k)(1) Military and Veterans Activities Covered entities may disclose PHI of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes that are permitted for Armed Forces personnel and under the same conditions.	Do you ever disclose PHI of individual who are foreign military personnel?	obtain copy of policy/procedure			
46	(k)(2) National Security and Intelligence Activities Such disclosure is allowed if the national security activities are authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).	Do you ever disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities?	obtain copy of policy/procedure			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
47	(k)(3) Protective Services for the President and Others Such disclosure is allowed for the protective services of the President and other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and B79	Do you ever disclose PHI to authorized federal officials for the provision of protective services to the President or other persons?	obtain copy of policy/procedure			
48	(k)(4) Medical Suitability Determinations These covered entities may use PHI to make medical suitability determinations and may disclose whether or not the individual was found to be suitable to officials in the Dept. of State for specified purposes. (See the regulation for these purposes).	This is only applicable to covered entities who are a component of the Department of State.	obtain copy of policy/procedure			
49	(k)(5) Correctional Institutions and Like Law Enforcement Entities This disclosure is allowed if the institution or official represents such PHI is necessary for the provision of health care to the individual, the health and safety of the individual, other inmates, officers or employees of the institution, or persons transporting the individual; law enforcement on the premises of the institution; and administration and maintenance of the safety, security, and good order of the institution.	Do you ever disclose to a correctional institution or law enforcement official having lawful custody of an inmate or other individual, PHI about the inmate or individual?	obtain copy of policy/procedure			
D. Opportunity to Agree or Reject with Uses of Information is NOT Required...(cont)						
	164.512(c)-(l) Other (cont)					
50	(k)(6) Government Programs Providing Government Benefits Disclosure of PHI relating to eligibility for enrollment is allowed to another government agency if the sharing of such information is in a single or combined data system accessible to all such government agencies and is required or authorized by state or regulation, or if the programs serve similar or same populations and the disclosure is necessary to coordinate the functions of such programs.	This is only applicable to covered entities that are health plans that are government programs providing public benefits or government agencies that administer a government program providing public benefits.	obtain copy of policy/procedure			
51	(l) Workers' Compensation Such disclosure is allowed to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.	Do you ever disclose PHI to workers' compensation or other similar programs?	obtain copy of policy/procedure			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
E. Other Requirements Related to Use and Disclosure of Health Info						
	Section 164.514 Other requirements relating to uses and disclosures of protected health information					
	164.514(a) - (c) Identification of PHI					
52	(a) and (b) De-identification of PHI This type of information is not considered to be individually identifiable health information and therefore is not subject to the requirements of the regulation. However, there are requirements to be met to ensure the PHI is de-identified. (See regulation for requirements).	Do you ever use or disclose health information that does not identify an individual and where there is no reasonable basis to believe the individual can be identified?	obtain copy of policy/procedure			
53	(c) Reidentification of PHI A covered entity may assign a code or other means of record identification to re-identify information provided that the code or record identification is not derived from information related to the individual or otherwise capable of being translated to identify the individual; and the covered entity does not use or disclose the code or other record identification for any other purpose, and does not disclose the mechanism for re-identification.	If you use de-identified information, do you ever have a need to re-identify the information?	obtain copy of policy/procedure			
	164.514(d) Minimum Necessary Requirements					
54	(d)(1) Standard The regulation required that when using or disclosing PHI, or requesting PHI from another covered entity, reasonable efforts are made to limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Note: This minimum necessary standard does not apply to disclosures to a provider for treatment and other exceptions as noted in the regulation (164.502(b)(2).	Do you have policies and procedures that allow for making reasonable efforts to limit PHI to the minimum necessary to accomplish the purpose for which it is needed?	obtain copy of policy/procedure			
55	(d) Minimum Necessary Uses and Disclosures A covered entity must identify persons or classes of persons in the workforce who need access to PHI to carry out their duties. Also, for each person/class of person, the entity must identify and make reasonable efforts to limit that access to the category or categories of PHI to which access is needed and any conditions appropriate to such access.	Do you have policies and procedures that identify your workforce members who need access to protected health information to carry out their duties?	obtain copy of policy/procedure			
E. Other Requirements Related to Use and Disclosure of Health Info (cont)						
	164.514(e) - (h) Other Requirements					

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
56	(e) Marketing A covered entity may use PHI for marketing purposes without an authorization if the marketing communication meets certain conditions. (See regulation for the list of conditions.)	Do you use PHI for marketing purposes?	obtain copy of policy/procedure, interview public relations, marketing			
57	(f) Fundraising A covered entity may use PHI for fundraising purposes without an authorization if the use or disclosure meets certain conditions. (See regulation for the conditions.)	Do you use PHI for fundraising purposes?	obtain copy of policy/procedure, interview public relations, marketing			
58	(g) Underwriting and Related Purposes If a health plan receives PHI for the listed purposes, and if such health insurance or health benefits are not placed with the plan, such health plan may not use or disclose the PHI for any other purpose, except as may be required by law.	Do you PHI for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits?	obtain copy of policy/procedure, interview HIM			
59	(h) Verification Requirements The covered entity must verify the identity and authority of persons requesting PHI and obtain any required documents for the disclosure, except for disclosures requiring and opportunity for the individual to agree or object. (See regulation for the implementation specifications related to verification procedures.)	Do you have policies and procedures in place to verify the identity and authority of persons requesting PHI and for obtaining any documentation, statements, or representation that is a condition of a disclosure?	obtain copy of policy/procedure			

F. Notice of Privacy Practices

	Section 164.520 Notice of privacy practices for protected health information					
60	(a) Standard Other than certain exceptions for group health plans and inmates, individuals have rights to adequate notice of the use and disclosures of their PHI that may be made. (See the regulation for a description of these exceptions.)	Do you have a process to provide adequate notice to individuals of the uses and disclosure of PHI that you may make, and of their rights and your legal duties with respect to PHI?	obtain copy of policy/procedure, interview admitting/registration			
61	(b)(1) Content of Notice The covered entity must provide a notice that is written in plain language and that contains specified elements. (See regulation for the required elements.)	Does your process provide a notice that contains the required elements?	obtain copy of policy/procedure, interview admitting/registration			
62	(b)(viii)(3) Revisions to Notice When there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice, the covered entity must promptly revise and distribute its notice. (Except where required by law, such a change may not be implemented prior to the effective date of the notice in which the change is reflected.)	Does your process provide for revisions of the notice and distribution of the changes?	obtain copy of policy/procedure, interview admitting/registration			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
63	(c)(1) and (2) Requirements for Health Plans and Certain Covered Providers There are specific requirements for health plans and for certain covered health care providers related to the provision of the notice to individuals. (See regulation for the requirements.)	If applicable, do your processes meet the specific requirements for health plans or for health care providers that have a direct treatment relationship with an individual?	obtain copy of policy/procedure			
64	(c)(3) Requirements for Electronic Notice A covered entity that provides information about its customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site. (See regulation for the further provisions of electronic notice).	Do you maintain a web site that provides information about your customer services or benefits?				
65	(d) Joint Notice by Separate Covered Entities Covered entities that participate in organized health care arrangements may comply with notice requirements by a joint notice if the joint notice meets certain conditions. (See regulation for these conditions)	Do you participate in any organized health care arrangements?				
66	(e) Documentation A covered entity must document compliance with the notice requirements by retaining copies of the notices it issues for six years from the date of its creation or the date when it last was effective, whichever is later.	Do you have process in place to document compliance with the notice?	interview administrative staff			
G. Right to Request Restrictions of Uses and Disclosures						
Section 164.522 Rights to request privacy protection for protected health information						
67	(a)(1) Restriction of Uses and Disclosures A covered entity must permit an individual to request a restriction, however a covered entity is not required to agree to a restriction. If the restriction is agreed to, the entity may not violate the restriction except to provide emergency treatment. If this occurs, the entity must request that the provider to further disclose the information. Such a restriction is not effective to prevent use or disclosure permitted or required for treatment (164.502(a)(2)(i), for facility directions (164.510(a), or for which consent, authorization, or opportunity to agree/object is not required (164.512)	Do you have a process in place to allow individuals to request restrictions for PHI for treatment, payment, or health care operations, or for any disclosures permitted for involvement in care and notification purposes which require an opportunity to agree or object (164.510(b)?	interview admitting/registration, ED, risk management			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
68	(a)(2) Terminating a Restriction Covered health care providers must permit individuals this request and must accommodate reasonable requests. Covered health plans must also permit and accommodate such requests, if the individual clearly states that the disclosure of all or part of the PHI could endanger the individual.	Do you have a process in place to allow for the termination of a restriction?	interview admitting/registration, ED, risk management, "grievance officer"			
69	(b)(1) Confidential Communication Requirements Covered health care providers care providers must permit individuals this request and must accommodate reasonable request. Covered health plans must also permit and accommodate such requests, if the individual clearly states that the disclosure of all or part of the PHI could endanger the individual.	Do you have a process in place to allow for individuals to request to receive (and to accommodate such requests) communications of PHI by alternative means or at alternative locations?	interview admitting/registration			
70	(b)(2) Conditions A covered entity may require the request in writing and may condition accommodation on information as to how payment, if any, will be handled (if appropriate) and specification of an alternative address or method of contact. A provider may not require an explanation as a basis for the request, but a health plan may require that a request contain a statement that the disclosure could endanger the individual.	Does your process allow for individuals to request to receive (and to accommodate such requests) communications of PHI by alternative means or at alternative locations meet the implementation specifications of the regulation?	interview HIM, RNs			
H. Patient Access to Protected Health Information						
	Section 164.524 Access of individuals to protected health information					
71	(a)(1) Right of Access Individuals have the right to access their own PHI with some exceptions. The entity may also deny access under certain circumstances. (See regulation for a description of the right of access and conditions for denial of access.)	Do you have a policy in place to allow individuals to inspect and obtain a copy of PHI about themselves?	obtain copy of policy/procedure, interview HIM, RNs			
72	(b) Timely Action A covered entity must act on a request for access no later than 30 days after the receipt of the request, with certain conditions for the actions. (See regulation for conditions)	Do you have a policy in place to allow for timely responses to a request for access?	obtain copy of policy/procedure, interview HIM			
73	(c) Provisions of Access A covered entity must comply with certain requirements when providing an individual with access, in whole or in part, to PHI. (See regulation for requirements)	When you grant a request for access, do your processes comply with the regulation's requirements?	obtain copy of policy/procedure, interview HIM			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
74	(d) Denial of Access A covered entity must comply with certain requirements when denying an individual access in whole or in part, to PHI. (See regulation for requirements)	When you deny a request for access, do your processes comply with the regulation's requirement	obtain copy of policy/procedure, interview HIM			
75	(e) Documentation A covered entity must document the designated record sets that are subject to access by individuals and the titles of the persons or offices responsible for receiving and processing requests for access by individuals. Such documentation must be retained for 6 years from time of creation or last effective date, whichever is later.	Does your policy regarding provisions for access and denial of access include documentation and retention requirements?	obtain copy of policy/procedure, interview HIM			
I. Amendment of Protected Health Information						
Section 164.526 Amendment of protected health information						
76	(a) Right to Amend Individuals have the right to amend their PHI or records. The entity may also deny the requested amendment under certain circumstances. (See regulation for a description of the right to amend and conditions for denial of the amendment.)	Do you have a policy in place to allow individuals to amend PHI or a record about themselves?	obtain copy of policy/procedure, interview HIM, medical staff by-laws, administration			
77	(b) Requests and Timely Action A covered entity must act on a request for amendment no later than 60 days after the receipt of the request, with certain conditions for the actions. (See regulation for conditions.)	Do you have a policy in place to allow for timely responses to a request for amendment?	obtain copy of policy/procedure, interview HIM, medical staff by-laws, administration			
164.526(c) Accepting the Amendment						
78	(c)(1) Making the Amendment The appropriate amendment to the PHI or record must be made by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.	When you grant a request for amendment, do your processes comply with the regulation's requirements for making the amendment?	obtain copy of policy/procedure, interview HIM, medical staff by-laws, administration			
79	(c)(2) Informing the Individual The individual must be informed timely that the amendment is accepted, and the entity must obtain the individual's identification of and agreement to have the entity notify the relevant persons with which the amendment needs to be shared.	When you grant a request for amendment, do your processes comply with the regulation's requirements for informing the individual?	obtain copy of policy/procedure, interview HIM, medical staff by-laws, administration			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
80	(c)(3) Informing Others A reasonable effort must be made to inform and provide the amendment, within a reasonable time, to persons identified by the individual as having received PHI and needing the amendment, and persons (including business associates) that the entity knows have the PHI that is subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.	When you grant a request for amendment, do your processes comply with the regulation's requirements for informing others?	obtain copy of policy/procedure, interview HIM, medical staff by-laws, administration			
I. Amendment of Protected Health Information (cont)						
	164.526(d) Denying the Amendment					
81	(d)(1) Denial A covered entity must comply with certain requirements when denying a request for amendment, in whole or in part, to PHI. (See regulation for requirements)	When you deny a request for amendment, do your processes comply with the regulation's requirements for denial?	obtain copy of policy/procedure, interview HIM, medical staff by-laws, administration			
82	(d)(2) Statement of Disagreement The entity must permit the individual to submit to the entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of the statement of disagreement.	Does your policy regarding denial of a a request for amendment allow for a statement of disagreement from the individual?	obtain copy of policy/procedure, interview HIM, medical staff by-laws, administration			
83	(d)(3) Rebuttal Statement The entity may prepare a written rebuttal to the individual's statement of disagreement. A copy of such a rebuttal must be provided to the individual who submitted the statement of disagreement.	Does your policy regarding denial of a request for amendment allow for a rebuttal to a statement of disagreement from the individual?	obtain copy of policy/procedure, interview HIM, medical staff by-laws, administration			
84	(d)(4) Recordkeeping The covered entity must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link all the documents listed to the left to the designated record set.	Does your policy regarding denial of a request for amendment allow for the record keeping of the request for amendment, the denial of the request, the statement of disagreement, and the rebuttal?	obtain copy of policy/procedure, interview HIM, medical staff by-laws, administration			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
85	(d)(5) Future Disclosures If a statement of disagreement has been submitted the entity must include, with the material appended in the recordkeeping requirement, an accurate summary of any such information with subsequent disclosures of the PHI involved. If there is not statement of disagreement, the entity must include the request for amendment and denial or summary thereof with subsequent disclosures of the PHI involved. If the disclosure is being made using a standard transaction that does not permit the additional material, the covered entity may separately transmit the additional material.	Does your policy regarding denial of a request for amendment allow for future disclosures which include the information about the disagreement?	obtain copy of policy/procedure, interview HIM, medical staff by-laws, administration			
I. Amendment of Protected Health Information (cont)						
86	(e) Actions on Notices of Amendment A covered entity that is informed by another covered entity of an amendment to an individual's PHI, must amend the PHI in designated record sets.	Do you have a process for amending an individual's PHI when you are informed by another covered entity of an approved amendment?	interview HIM, RNs, medical staff by-laws			
87	(f) Documentation A covered entity must document the titles of the persons or offices responsible for receiving and processing requests from individuals for amendments and retain the documentation for 6 years from date of creation or last effective date, whichever is later.	Do you document the titles of the persons or offices responsible for receiving and processing requests for amendments?	interview HIM, RNs, medical staff by-laws			
J. Accounting of Disclosures						
	Section 164.528 Accounting of Disclosures of Protected Health Information					
88	(a) Right to an Accounting of Disclosures Individuals have the right to receive an accounting of disclosures of PHI made by a covered entity in the six years prior to the date on which the accounting is requested, with some disclosures excepted. (See regulation for exceptions.)	Do you have processes in place to provide individuals with an accounting of disclosures of PHI made by you in the six years prior to the date on which the accounting is requested?	interview HIM, Business office/Patient Accounts			
89	(b) Content of the Accounting There are specific requirements for the content of the accountings given in response to a request. (See regulation for these requirements.)	Do the accountings you provide in response to requests by individuals for accountings of disclosures meet all the requirements of the regulations?	obtain copy of policy/procedure, interview HIM, Business office/Patient Accounts			
90	(c) Provision of the Accounting The covered entity must act on the individual's request no later than 60 days after receipt of such request, following certain conditions (See regulation for conditions).	Do your provisions of requested accountings meet the timeliness requirements?	obtain copy of policy/procedure, interview HIM, Business office/Patient Accounts			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
91	(d) Documentation A covered entity must document the information required to be included in the accounting (content), the written accounting that is provided, and the titles of the persons or offices responsible for receiving and processing request of an accounting. This documentation must be retained for 6 years from the date of creation or the last effective date, whichever is later.	Does your policy regarding provisions for accounting include documentation and retention requirements?	obtain copy of policy/procedure, interview HIM, Business office/Patient Accounts			
K. Administrative Requirements						
	Section 164.530 Administrative Requirents					
92	(a) Personnel Designations Covered entities must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity, and a contact person or office who is responsible for receiving complaints and who is able to provide further information about matters covered by the required notice.	Does your entity have a designated privacy official?	obtain copy of job description-- human resources			
93	(b) Training A covered entity must train all members of its workforce on the policies and procedures relating to PHI, as necessary and appropriate for the workforce to carry out their function within the entity. Training must be given no later than the entity's compliance date, thereafter, to each new member of the workforce in a reasonable time frame, to each member whose functions are affected by a material change in the policies and procedures within a reasonable time frame, and the entity must document that the training has been provided.	Does your entity have a program in place to provide training as required by the regulation?	interview administrative staff, human resources			
94	(c) Safeguards A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the PHI from any intentional or unintentional use or disclosure that is in violation of the regulation.	Does your entity have appropriate safeguards in place to protect the privacy of PHI?	interview administrative staff, HIM, IT...walk through			
95	(d) Complaints to the Covered Entity A covered entity must provide a process for individuals to make such complaints and must document all complaints received, and their disposition, if any. This documentation must be retained for 6 years from the date of creation or the last effective date, whichever is later.	Do you have a process in place for individuals to make complaints concerning your policies and procedures that are required by the regulation or your compliance with such policies and procedures or any requirements of regulation?	interview administrative staff, compliance officer			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
96	(e) Sanctions Covered entities are required to have such a sanction policy and must document the sanctions that are applied, if any. The sanction requirement does not apply to a member of the workforce who used or disclosed PHI that is permitted by the regulation (under 164.502) or meets the conditions for refraining from intimidating or retaliatory acts.	Do you have a sanction policy in place to respond to members of your workforce who fail to comply with your privacy policies and procedures or the requirements of the regulation?	interview administrative staff, human resources, department managers			
97	(f) Mitigation A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the entity of a use or disclosure in violation of its policies and procedures or the requirements of the regulation.	Do you have a policy in place regarding mitigation of any harmful effect that may have occurred as a result of a use or disclosure of PHI in violation of your policies and procedures or the requirements of the regulation.	interview administrative staff, human resources, department managers			
K. Administrative Requirements (cont)						
	Section 164.530 Administrative Requirements					
98	(g) Refraining from Intimidating or Retaliatory Acts A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who exercised his/her rights as provided by the regulation, and individual or other person for filing a complaint with the Secretary, testifying, assisting, or participating in an investigation compliance review, proceeding, or hearing, or for opposing any act or practice made unlawful by the regulation.	Do you have an non-retaliation policy in place?	obtain copy of policy/procedure, interview administrative staff, department managers, risk management			
99	(h) Waiver of Rights A covered entity may not require individuals to waive their rights to file a complaint (160.306) or as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.	Do any of your policies or procedures, intentionally or unintentionally require individuals to waive their rights to file a complaint of as condition to treatment, payment, enrollment in a health plan, or eligibility for benefits.	obtain copy of policy/procedure, interview administrative staff, department managers, risk management, compliance/complaint			
100	(i) Policies and Procedures A covered entity must implement policies and procedures with respect to PHI that are designed to comply with the standard, implementation specifications, or other requirements of the regulation. A covered entity must change its policies and procedures as necessary and appropriate to comply with change in the law. (See the regulation for the requirements related to policies and procedures and their changes).	Do you have policies and procedures in place that are designed to comply with the requirements of the regulation and a process in place for making and implementing changes to these policies and procedures.	obtain copy of policy/procedure, interview administrative staff, department managers, risk management, compliance/complaint			

DMH HIPAA Privacy Assessment Tool

Disclaimer: The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice. The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance. Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Interim Privacy Officer, Missouri Department of Mental Health, 314.877.0123.

Q#	Section/Regulation	Question/Considerations	Obtain copy and/or Staff to interview	Comments or Assessment	Policy: 1=Centralized	Policy Name/Number (Source)
101	(j) Documentation A covered entity must maintain the required policies and procedures in written or electronic form, any required written communications in written or electronic form, and documentation of any required action, activity or designation in written or electronic form, for the required time period.	Do your documentation procedures require you to maintain all required documentation, and to retain it for 6 years from the date of its creation or the date when it last was in effect, whichever is later?	obtain copy of policy/procedure, interview administrative staff, department managers, risk management, compliance/complaint			
102	(k) Group Health Plans A group health plan is not subject to the standard or implementation specifications for personnel designations, training, safeguards, complaints, sanctions, mitigation, and policies and procedures if it meets certain requirements. See the regulation for these requirements.	Is your entity a group health plan that may be exempt from many of the administrative requirements?	obtain copy of policy/procedure, interview administrative staff, department managers, risk management, compliance/complaint			